



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/759,636	01/16/2004	Monica Ene-Pietrosanu	MS1-1762US	1219
22801	7590	06/04/2007	EXAMINER	
LEE & HAYES PLLC 421 W RIVERSIDE AVENUE SUITE 500 SPOKANE, WA 99201			KIM, JUNG W	
			ART UNIT	PAPER NUMBER
			2132	
			NOTIFICATION DATE	DELIVERY MODE
			06/04/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lhptoms@leehayes.com

Office Action Summary	Application No.		Applicant(s)	
	10/759,636		ENE-PIETROSANU ET AL.	
	Examiner		Art Unit	
	Jung Kim		2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-40 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-40 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____. |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date ____. | 6) <input type="checkbox"/> Other: ____. |

DETAILED ACTION

1. Claims 1-40 are pending.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 16-29, 31 and 35-40 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 16-28 recites a computer readable medium having computer-implementable instructions. The specification discloses that a computer-readable media may include application programs, other program modules and program data. Pg. 9, lines 7-19. Claims 29-40 recites an apparatus. The specification discloses that an apparatus may be implemented within one or more application programs, other program modules, and/or program data. Pg. 9, lines 20-22. However, application programs, program modules and program data per se are not recognized as one of the four statutory classes of invention.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

Art Unit: 2132

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-7, 10-21, 23-33 and 35-40 are rejected under 35 U.S.C. 102(b) as being anticipated by Elgamal et al. USPN 6,397,330 (hereinafter Elgamal).

6. As per claims 16-21, 23-28, Elgamal discloses a computer readable medium having computer-implementable instructions for causing one or more processing units to perform acts comprising:

- a. selectively detecting a request for at least one cryptography service; and selectively performing at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy at least one cryptography service parameter threshold; (Col. 5:60-6:4; 6:19-37)
- b. establishing said at least one cryptography service parameter threshold; (5:62-63; 6:25-27 and lines 53-55; 7:11-28)
- c. wherein establishing said at least one cryptography service parameter threshold includes at least one of the following acts: identifying unacceptable

cryptography algorithms; and identifying acceptable cryptography algorithms (6:26-27 and lines 57-60; 7:15-17 and lines 22-28);

d. wherein establishing said at least one cryptography service parameter threshold includes at least one of the following acts: identifying at least one unacceptable cryptography key size parameter; and identifying at least one acceptable cryptography key size parameter (5:66-6:2; 6:25-31 and lines 53-56);

e. wherein establishing said at least one cryptography service parameter threshold includes establishing a plurality of correctness categories, wherein each at least one of said plurality of correctness categories includes at least one cryptography algorithm identifier (6:57-65; 8:1-34 "Table 2");

f. wherein said plurality of correctness categories includes at least one correctness category selected from a group of correctness categories comprising authorized algorithms, unauthorized algorithms, weak algorithms, and strong algorithms (5:66-6:2; 6:25-37);

g. wherein selectively detecting said request for at least one cryptography service includes monitoring at least one process selected from a group of processes comprising an application, an operating system, a cryptography algorithm, and a cryptography application programming interface. (5:60-61; 6:19-21)

h. wherein selectively performing said at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy said at least one cryptography service

parameter threshold includes determining if a cryptographic key associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold (6:2; 6:25-31);

i. wherein determining if said cryptographic key associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold includes comparing a size of said cryptographic key with said at least one cryptography service parameter threshold (6:2; 6:25);

j. wherein selectively performing said at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy said at least one cryptography service parameter threshold includes determining if a cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold (5:66-6:4; 6:25-35; 7:15-20);

k. wherein determining if said cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold further includes comparing a cryptography algorithm identifier with said at least one cryptography service parameter threshold (5:66-6:4; 6:25-35; 7:15-20);

l. wherein selectively performing said at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy said at least one cryptography service

parameter threshold includes performing at least one action selected from a group of actions comprising interrupting at least one process, stopping at least one process, starting at least one process, displaying alert information, logging alert information, suggesting at least one alternative cryptography service, outputting alert messages, causing alteration of a graphical user interface, and forcing use of at least one other cryptography service (6:3-4, 30 and lines 57-60).

7. As per claims 1-7 and 10-15, they are method claims corresponding to claims 16-21 and 23-28, and they do not teach or define above the information claimed in claims 16-21 and 23-28. Therefore, claims 1-7 and 10-15 are rejected as being anticipated by Elgamal for the same reasons set forth in the rejections of claims 16-21 and 23-28.

8. As per claims 29-33 and 35-40, they are apparatus claims corresponding to claims 16-21 and 23-28. In addition, Elgamal discloses cryptography correctness detection logic configured to perform the acts listed in claims 16-21 and 23-28, and moreover, Elgamal discloses memory operatively coupled to the correctness detection logic, wherein the cryptography service parameter threshold is in the memory. (fig. 1, "Policy Filters" and related text) As such, claims 29-33 and 35-40 are rejected as being anticipated by Elgamal.

9. Claims 16-18, 20, 21, 23, 26-31, 33, 35 and 38-40 are rejected under 35 U.S.C. 102(e) as being anticipated by Griffin et al. USPN 7,079,648 (hereinafter Griffin).

10. As per claims 1-3, 6, 7, 10, 13-18, 20, 21, 23 and 26-28, Griffin discloses a computer readable medium having computer-implementable instructions for causing one or more processing units to perform acts comprising:

m. selectively detecting a request for at least one cryptography service; and selectively performing at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy at least one cryptography service parameter threshold; (Col. 5:1-41)

n. establishing said at least one cryptography service parameter threshold; (5:4-5 and lines 50-55; 7:29-45)

o. wherein establishing said at least one cryptography service parameter threshold includes at least one of the following acts: identifying unacceptable cryptography algorithms; and identifying acceptable cryptography algorithms (5:50-58; 7:21-45);

p. wherein establishing said at least one cryptography service parameter threshold includes establishing a plurality of correctness categories, wherein each at least one of said plurality of correctness categories includes at least one cryptography algorithm identifier (5:4-5 and lines 50-55);

q. wherein said plurality of correctness categories includes at least one correctness category selected from a group of correctness categories comprising authorized algorithms, unauthorized algorithms, weak algorithms, and strong algorithms (5:5-7; 7:29-62);

- r. wherein selectively detecting said request for at least one cryptography service includes monitoring at least one process selected from a group of processes comprising an application, an operating system, a cryptography algorithm, and a cryptography application programming interface. (5:1-5)
- s. wherein selectively performing said at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy said at least one cryptography service parameter threshold includes determining if a cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold (7:21-62);
- t. wherein determining if said cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold further includes comparing a cryptography algorithm identifier with said at least one cryptography service parameter threshold (7:21-62);
- u. wherein selectively performing said at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy said at least one cryptography service parameter threshold includes performing at least one action selected from a group of actions comprising interrupting at least one process, stopping at least one process, starting at least one process, displaying alert information, logging alert information, suggesting at least one alternative cryptography service,

outputting alert messages, causing alteration of a graphical user interface, and forcing use of at least one other cryptography service (5:17-47).

11. As per claims 1-3, 6, 7, 10 and 13-15, they are method claims corresponding to claims 16-18, 20, 21, 23 and 26-28, and they do not teach or define above the information claimed in claims 16-18, 20, 21, 23 and 26-28. Therefore, claims 1-3, 6, 7, 10 and 13-15 are rejected as being anticipated by Griffin for the same reasons set forth in the rejections of claims 16-18, 20, 21, 23 and 26-28.

12. As per claims 29-31, 33, 35 and 38-40, they are apparatus claims corresponding to claims 1-3, 6, 7, 10 and 13-15. In addition, Griffin discloses cryptography correctness detection logic configured to perform the acts listed in claims 1-3, 6, 7, 10 and 13-15, and moreover, Griffin discloses memory operatively coupled to the correctness detection logic, wherein the cryptography service parameter threshold is in the memory. (fig. 1, reference nos. 110 and 200, and fig. 5 'System memory' and related text) As such, claims 29-31, 33, 35 and 38-40 are rejected as being anticipated by Griffin.

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

14. Claims 8, 9, 22 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Elgamal in view of Fielder et al. USPN 5,963,646 (hereinafter Fielder).

15. As per claim 22, the rejection of claim 17 under 35 USC 102(b) as being anticipated by Elgamal is incorporated herein. In addition, Elgamal discloses disabling a crypto module if the module does not correctly implement the algorithms and/or key sizes configured, and removing unauthorized cipher suites, wherein a cipher suite is a collection of encryption algorithms, key sizes, and parameters that specifies the type and strength of a particular cryptographic operation. (Col. 5:66-6:5; 6:25-31) Elgamal does not expressly disclose, wherein establishing said at least one cryptography service parameter threshold includes at least one of the following acts: identifying at least one acceptable seed size parameter; and identifying at least one unacceptable seed size parameter. However, it is well known in the art at the time of invention that the length or size of a seed value, which is used to generate a cryptographic key directly corresponds to the cryptographic strength of the key value used in a cipher function. For example, Fielder discloses a key generator that takes as inputs one or more seed values to generate a deterministic encryption key. Fig. 2. Fielder further discloses that the size of the seed value has a direct relationship to the strength of the generated encryption key. Col. 5:54-6:4. Hence, a seed value is a significant parameter that specifies the type and strength of a particular cryptographic operation. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the act of establishing

Art Unit: 2132

the at least one cryptographic service parameter threshold as disclosed by Elgamal to include at least one of the following acts: identifying at least one acceptable seed size parameter; and identifying at least one unacceptable seed size parameter. One would be motivated to do so because seed size directly corresponds to the strength of a particular cryptographic operation as taught by Fielder and as known to one of ordinary skill in the art. The aforementioned covers the limitation of claim 22.

16. As per claims 8 and 9, they are method claims corresponding to claim 22, and they do not teach or define above the information claimed in claim 22. Therefore, claims 8 and 9 are rejected as being unpatentable over Elgamal in view of Fielder for the same reasons set forth in the rejection of claim 22.

17. As per claim 34, it is an apparatus claims corresponding to claims 22 and 30, and it does not teach or define above the information claimed in claims 22 and 30. Therefore, claim 34 is rejected as being unpatentable over Elgamal in view of Fielder for the same reasons set forth in the rejection of claim 22 and 30.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

Art Unit: 2132

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Jung Kim
Examiner AU 2132
May 26, 2007